REMARKS/ARGUMENTS

Claims 1-3 have been amended, claim 4 was previously canceled, claim 5 is currently canceled, and claims 6-9 have been amended to more clearly define Applicant's invention in the terms of Applicant's disclosures. Applicant submits that his amended claims now meet the requirements of 35 USC § 112, overcome the objections under 35 USC § 102, and define patentably over Garib (U. S. Patent 6,728,378 hereinafter "Garib").

The Rejection of Claims 1-3 and 5-9 under 35 USC § 112, First Paragraph

Two of the Examiner's Findings Need Clarification

The Examiner asserts that Applicant's specification discloses that "... a "web site" is a network server ..." (current Office Action page 3 lines 4-5). But Applicant's specification contains no such disclosure. In fact, the term "network server" is not used anywhere in Applicant's entire application. It is commonly known that the term "web site" refers to a collection of web site HTML documents that are stored in a network server's storage system, and does not refer to the network server itself.

The examiner also asserts that Applicant's specification discloses that "... a "page" is a downloaded document created using HTML ..." (current Office Action page 3 lines 4-5). In fact, Applicant's specification discloses a "page" as a **web site HTML document** (current application page 4 lines 28-29) to clearly distinguish it from other types of HTML documents, such as those used by Garib, which do not have the same operating characteristics.

Applicant submits that a proper evaluation of his invention could not be made in light of the above confusion, particularly as it pertains to Applicant's arguments for allowance under 35 USC § 102(e).

Claims Have Been Changed to Clarify Applicant's Defined Subject Matter

In general, the Examiner's findings which are argued throughout the current Office Action indicate that Applicant's claims have not previously defined Applicant's subject matter clearly. Accordingly, extensive claim amendments have been made to clarify the definitions in Applicant's claims with respect to their associated disclosures. This is discussed in more detail in the following arguments.

Applicant's Arguments

Claim 1 was rejected because the Examiner has determined that the following elements and methods were not disclosed in Applicant's specification --

With respect to "web site page" (current Office Action page 3 line 6) –

The term "web site page" has been replaced in Applicant's amended claims which now define a "web site HTML document" as disclosed by Applicant (current application page 4 lines 28-29) and shown in the current application in Figs. 1-A and 6, and using Ref.# 100 in Figs. and in their associated text as "page".

With respect to "validating an associated key" (current Office Action page 3 line 10-11) –

The term "associated key" has been replaced in Applicant's amended claims which now define it as a "viewer-entered clear-text key" as disclosed in Applicant's specification (current application, page 4 lines 30-31) and called "showkeys" for brevity (current application Figs. 6, 3-B, and 7-A & B) and as Ref.# 3XX in the Figs., and in the associated text disclosures.

With respect to "automatically activate" –
Amended Claim 1 no longer contains the term "automatically activate."

With respect to "execute within the confines" –
Amended Claim 1 no longer contains the phrase "execute within the confines."

The Examiner includes a paragraph (Current Office Action page 4 lines 3-9) in which are listed the assumptions made for examination purposes with respect to the four above-referenced phrases used in Applicant's Claim 1. These assumptions have already been considered in Applicant's above explanations and amendments with respect to Claim 1.

Dependent claims

The current Office Action contains no arguments for rejecting dependent claims 2 and 3 under 35 USC § 112, first paragraph. Dependent claim 4 is previously canceled, and dependent claim 5 is canceled

Dependent Claim 6 was rejected because the Examiner has determined that the following methods were not disclosed in Applicant's specification --

With respect to "human operator provides said plurality of said associated keys" –
The term "human operator" has been replaced in Applicant's amended claims which now use the term "viewer" that is currently disclosed (current application Figs. 6, 4-B, and 7-B, and 7-C), using Ref.# 4XX in the Figs. and in their associated text. The term "associated key" has been replaced in Applicant's amended claims which now use the term "viewer-entered clear-text key" as in amended claim 1 above.

With respect to "human operator determines which of said plurality of said cryptograms are decrypted" –
Claim 6 is amended and no longer includes the above phrase.

The current Office Action contains no specific arguments under 35 USC § 112, first paragraph, for rejecting dependent claims 7-9.

All of Applicant's claims have either been amended to overcome the § 112 rejection or canceled. As a result, Applicant's disclosures are now in compliance with 35 USC § 112, first paragraph. Applicant therefore requests reconsideration and withdrawal of the rejection of claims 1 and 6 under 35 USC § 112, first paragraph.

The Rejection of Claims 1-3 and 5-9 under 35 USC § 112, Second Paragraph

Applicant's Arguments

Claim 1 was rejected because it fails to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

With respect to the phrase in Claim 1 which reads "... execute within the confines ..." as referenced by the Examiner (current Office Action page 5 lines 8-12) –

Claim 1 is amended to omit the term "... execute within the confines ..." as mentioned in Applicant's arguments under 35 USC § 112, first paragraph.

Dependent Claims 2, 3 and 5 – 9 were rejected at least by virtue of their dependency on the dependent (SIC) claims (current Office Action page 5 lines 16-17). –

In addition to independent Claim 1, all dependent claims are either canceled or amended to properly define Applicant's invention.

As a result of the cancellation of claim 5 and the amendments to the remainder of Applicant's claims, they are now in compliance with 35 USC § 112, second paragraph. Applicant therefore requests reconsideration and withdrawal of the rejection of all claims under 35 USC § 112, second paragraph.

The Patentability of Currently Amended Claims 1-3 and 6-9 under 35 USC § 102 (e)

As is well known, under 35 USC § 102 (e), anticipation requires that each and every element of the claimed invention be disclosed in one prior art reference. Applicant submits that each and every element of the amended claims is not found in Garib, and that Claims 1-3 and 6-9 are now patentable.

Garib's and Applicant's HTML Documents are Not the Same

While Garib discloses that his "... messages may be formatted in hypertext markup language (HTML) ..." (Garib column 2 lines 30-40), it should also be noted that Garib's method discloses the transmission of only one private message at a time (Garib column 12 line 46 to column 13 line 59) using one HTML document (such as an email delivery), and does not disclose the transmission of multiple private messages using multiple HTML documents at the same time (such as a web site visit).

Unlike Garib, Applicant discloses a method which requires the use of a web site HTML document (current application page 4 lines 28-29). It is well known that Garib's single HTML document does not have the same operating characteristics as the web site HTML document called for in Applicant's method. One feature attributed only to Applicant's web site HTML documents is that they can exchange data with each other after they are downloaded from the same web site. This important capability is vital to the implementation of Applicant's many novel features and benefits which cannot possibly be implemented in Garib's stand-alone HTML document, and indeed, he does not define Applicant's features.

Garib's and Applicant's Subject Matters are Not the Same

Scope and Purpose --
Garib's invention is a method for combining and using known software elements to provide an entire system for securely transmitting personal and private information to those to which it belongs. The information is sent as email or a similarly transmitted document, and is decrypted when received. This type of Internet system is in common use today at the **enterprise level** for protecting the interests of the **person receiving the information**.

Applicant's disclosures are solely devoted to a method for constructing only a decryption **function** that could be **added** to any **existing web site system,** giving it the capability to selectively and securely distribute different private messages to different site visitors. Applicant's invention principally protects the interests of the **web site publishers who send the information**.

Method Disclosure --
Although Garib discloses the availability of two existing decryption **algorithms** that could be used in his invention (Garib column 4 lines 27-42), he does not disclose any method whatsoever for integrating any decryption algorithm with his other system elements in a way that would construct a decryption **function** that operates as claimed.

> Applicant's invention is solely dedicated to a method for interfacing and operating a decryption function in concert with all of the other elements required for a fully-featured and document-resident decryption capability. Accordingly, Applicant completely teaches the method in the form of environmental and software flow charts with their supporting text and the script code which can be used to implement the invention.

Applicant's claims and Garib's disclosures show their inventions to be different in scope, purpose, operational features, benefits, and method. It is clear that Garib does not describe Applicant's invention at any level.

In light of the above, Applicant submits that all of Applicant's currently amended Claims 1-3 and 6-9 are patentable over Garib under 35 USC § 102(e).

Applicant's Arguments for Acceptance of Currently Amended Claims

Claim 1 is not anticipated by Garib

A method for decrypting a plurality of cryptograms which are placed within each web site HTML document in a plurality of web site HTML documents that are being downloaded from a web site by a viewer that is visiting said web site, comprising:

(a) providing said plurality of web site HTML documents,

Garib does not make any disclosure whatsoever to suggest that web site HTML documents, singly or in a plurality, are used in his method for transmitting an encrypted message (Applicant's cryptograms). Garib uses the term "web pages" twice in his Example 5 (Garib column 11 lines 17-36), when he discloses the part of his system that registers a customer that will receive an encrypted message at a later time, but he does not use the term "web page" or any singular or plural equivalent in disclosing his method for receiving and decrypting a message.

(b) providing said plurality of cryptograms within each said web site HTML document,

Although Garib's independent claims and summaries refer to "encrypted messages" (Applicant's cryptograms) in the plural when defining or describing the general purpose of his invention, the disclosure of his decryption method refers only to a "message" in the singular (22 times), and furthermore, Garib does not disclose any method for receiving and processing more than one decrypted message in each transmission (Garib column 12 line 46 to column 13 line 59). Also, Garib does not disclose that his encrypted message is within a web site HTML document – please see the argument for element (a).

(c) providing the data within each said web site HTML document for validating a plurality of viewer-entered clear-text keys for said plurality of cryptograms,

Garib does not provide validating data within web site HTML documents – please see the argument for element (a). Also, Garib does not decrypt his password (Applicant's viewer-entered clear-text key) when it is entered, as called for in Applicant's method. In Garib's method, the password and the message are both validated together by the results of the final decryption process (Garib column 13 lines 35-59). Furthermore, Garib's method calls for only one password and one encrypted message (cryptogram) – please see the argument for element (b).

(d) providing an HTML frameset page for enabling data communications between said web site HTML documents,

Garib's specification does not contain the term "frameset" or "frameset page", nor does it contain any type of disclosure with respect to the use of a frameset page. This special, but well-known type of HTML document is used by Applicant in a novel way to provide for a single key-entry session that will distribute keys to all downloaded website pages in both framed and non-framed websites.

(e) providing a key handler function within each said web site HTML document for receiving and validating said plurality of viewer-entered clear-text keys,

Although Garib's method includes the entry of a password for each message to be decrypted, a careful examination of Garib finds no disclosure of a function for validating a password when it is received -- please see the argument for element (c). In Garib's method, the password is not determined to be valid until after the decryption process (Garib column 13 lines 50-59).

(f) providing a controller function within each said web site HTML document for activating and controlling said key handler function as needed, and

Since Garib's method provides for receiving only one password for each encrypted message that is received (please see the argument for element (c) above), his method does not include a function for controlling the repetitive operation of a key handler function.

(g) providing a decryption function within each said web site HTML document for generating a plurality of decrypted versions of said plurality of cryptograms that correspond to said plurality of viewer-entered clear-text keys that have been received and validated.

Garib's method does not include a method for decrypting a plurality of encrypted messages within the same transmitted document, nor does he include a method for applying validation information from more than one password to more than one cryptogram in the same transmitted document, nor does his method provide for the decryption of cryptograms in a document using passwords that have been received in a different document. Please see arguments for all Claim 1 elements above.

Dependent Claim 2 is not anticipated by Garib

The method of claim 1 wherein said plurality of decrypted versions will be made available for display in the original locations of said plurality of cryptograms.

Since Garib's method provides for only one private message per transmitted document (please see Claim 1 argument for element (b)), and since his message document contains only the encrypted message and supportive decrypting information (Garib Fig 1, Ref.# 117), his method does not address the concept of displaying a decrypted message in any particular location within the document display.

Dependent Claim 3 is not anticipated by Garib

The method of claim 1 wherein said plurality of cryptograms are any size up to the size allowed by HTML standards for the body of said web site HTML document.

No disclosures or claims can be found in Garib's specification that in any way address the allowed maximum and/or minimum size of his encrypted messages (Applicant's cryptograms). The words "size", "any size", "body", "allowed", and "HTML standards" are simply not used anywhere in Garib's specification or claims.

Dependent Claim 4 (previously canceled)

Dependent Claim 5 (canceled)

Dependent Claim 6 is not anticipated by Garib

The method of claim 1 wherein said viewer provides said plurality of viewer-entered clear-text keys, comprising:

(a) providing a first means for sending an input request to said viewer, and

(b) providing a second means for receiving said plurality of viewer-entered clear-text keys directly into said web site HTML document.

Although Garib discloses a process where future recipients of encrypted messages register their passwords (keys) with the bank (Garib column 11 lines 17-36), in the context of this disclosure, the term "passwords" has been used in association with the term "customers", and does not mean that each customer (recipient) provides more than one password when a message is received from the bank, particularly since each customer has previously registered only one password (Garib column 11 lines 37-41). Accordingly, Garib does not claim or disclose a method for receiving more than one password from a message recipient (Applicant's viewer) (please see Claim 1 argument for element (c)).

Dependent Claim 7 is not anticipated by Garib

The method of claim 6 wherein said viewer receives a validity report directly from said decryption function upon entry of each of said plurality of viewer-entered clear-text keys.

A careful reading of Garib discloses that a password is not validated when it is entered. He discloses only that (a) a correct password would either cause the message to be displayed properly or cause a message error alert (bad message), or (b) an incorrect password would either display the message as gibberish, or cause a message error alert (bad message) (Garib column 13 lines 50-59). Garib discloses no method for providing a validity report upon the entry of a password.

Dependent Claim 8 is not anticipated by Garib

The method of claim 1 wherein said plurality of viewer-entered clear-text keys are made available to each said web site HTML document in said plurality of web site HTML documents as each is being displayed.

Since Garib does not disclose the use of web site HTML documents or the use of a frameset page, Garib also does not anticipate the method for this claim in any way (please see Claim 1 arguments for elements (a) and (d)).

Dependent Claim 9 is not anticipated by Garib

The method of claim 1 wherein said controller function operates only on the first instance of said cryptogram being found within said web site.

Garib does not disclose a function for controlling the repetitive use of a decryption function, and he also does not provide for more than one cryptogram (please see Claim 1 arguments for elements (b) and (c)). Therefore, there is no concept of a "first instance of said cryptogram being found" provided for in his invention.

Applicant submits that none of the novel features in amended Claims 1-3 and 6-9 are found in Garib, much less each and every element. Applicant has persuasively argued that his amended claims are not anticipated by Garib.

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

By Ralph Bain, Applicant

Ralph Bain
39908 San Simeon Ct.
Fremont, CA 94539-3619
Tel.: (510) 657-6384